A Novel Video Steganography Algorithm Based on Trailing Coefficients for H.264/AVC

Yingnan Zhang, Minqing Zhang, Xu An Wang, Ke Niu and Jia Liu
Key Laboratory of Network and Information Security of CAPF, Electronic Department
Engineering University of the CAPF, Xi'an, Shaanxi, 710086, P. R. China
E-mail: zyn583@163.com, wangxazjd@163.com

Keywords: information security, video, steganography, trailing coefficients

Received: December 22, 2015

With the development of high-speed networks, life is more convenient than ever. However, the information security issue of high-speed networks is still a big problem. As an important branch of information security, steganography is a useful method to protect confidential information. In this paper, by combining the trailing coefficient produced in the process of the quantization ofthe H.264 encoding standard with the current video steganographic algorithms, we implement a new kind of algorithm based on trailing coefficients. The algorithm firstly conducts a DCT transform on the frame, and then it obtains the trailing coefficient for each quantized DCT block;lastly, the secret information bit is embedded into the video. The experimental result indicates that this algorithm has little influence on video quality and has a large capacity of steganography;also, it has a strong anti-steganalysis capability and high robustness.

Povzetek: Opisan je nov algoritem za video steganografijo.

1 Introduction

Currently, people are enjoying a high standard life due to the continuing growth of network bandwidth. In the past, people were unable to easily upload or share large digital content because of the bandwidth restrictions on networks. With the advancement of various technologies such as 4G/5G, the network speed has substantially increased, allowing people to share almost whatever they want. In this paper, we explore the concept of high bandwidth to design new video steganographic algorithms. As an important branch of information security, information hiding, also called steganography, has provided an efficient method to protect the security of sensitive information.

Steganography is a technique that can be used to transmit secret information publicly via digital media, while achieving covert communication [1]. There has been much advancement made in image steganography algorithms. However, because of the limited capacity of digital images, the capacity of secret information that can be embedded in the image is also restricted. Compared with a digital image, video has more advantages regarding steganography, such as it can support a larger capacity and there is more redundancy, a high communication quality, robustness, etc. As a new standard, H.264 has more advantages over the previous ones. There is a better compression of digital TV broadcasting, video real-time communication, network video streaming and multimedia messaging. Some of its biggest features are high reliability and high compression efficiency [2]. As a result, the study of steganographic methods based on video for H.264/AVC has become a popular research topic[3-8].

In the past, when video was transmitted on a network, it was transmitted by frames, like pictures, and an attacker would be able to observe the network's package transmitting. When an attacker would find many video frames in the network, he/she would pay attention to them; this situation,shown in Figure 1, is not an ideal situation for video steganography. Now, since there are very high-speed network and supported techniques [9-13], people can transmit video content easily. This does not gain the attacker's attention, as shown in Figure 2. It also satisfied the original intention of steganography-to hide the existence of secret information-so our algorithm can achieve a high security standard in networks when protecting sensitive information.

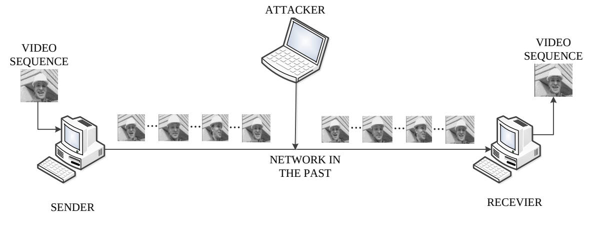


Figure 1: Transmitting video sequence in a network with low bandwidth.

When embedding secrets in the spatial domain, we found that it is easy to be detected by many steganalysis algorithms, so we chose to embed secrets in DCT coefficients. Furthermore, we believe that using the characteristic of the H.264 coding standard is a better choice because we can

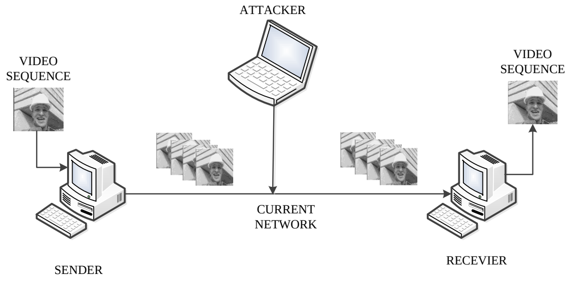


Figure 2: Transmitting video sequence in a current network.

embed secrets during the compression process. We save the time that being cost in embedding procession, thus reducing the complexity of our algorithm.

Hua et al. proposed a video steganography algorithm based on H.264/AVC [14]. The algorithm can be implemented to achieve good embedding and extracting, but the algorithm is weak when it is under attack. Langelaar proposed a mechanism for the compressed video stream [15]. The advantage of this algorithm is that it only needs part of the coding stream. As a result, this algorithm can achieve a higher data embedding capacity, but the algorithm is weak regarding anti-steganalysis detection. Ma proposed a novel algorithm based on H.264 [16],and it improves the visual quality, but the embedding efficiency and embedding capacity needs improvement. He also proposed a new method based on a motion vector [17], but the capacity of embedding is also limited. Zhang proposed a robust video watermarking algorithm for H.264/AVC based on texture features [18], it has little impact on the video quality and bit rate, but it can only achieve little capacity for embedding. Liu proposed a method based on macro-block segmentation [19], but the bit rate increase is very low, and it has weak anti-steganalysis detection. Ultimately, almost all of the steganography algorithms based on video for H.264/AVC exist some problems such as negative impacts on video quality, high complexity in embedding, and less capacity of embedding.

In this paper, we present a new video steganography algorithm by modifying trailing coefficients through certain rules to embed secret information. Experimental results showed that this algorithm has better visual invisibility, while improving the steganographic capacity, strong anti-steganalysis ability, and high robustness. Our algorithm's sketch is shown in Figure 3.

2 Trailing coefficients

Trailing coefficients are produced from CAVLC. By simply denoting, the trailing coefficient can be a number in the range of 0-3 and the amplitude can be 1. When the number of coefficients satisfying this condition is more than 3, we only choose the last three trailing coefficients; the other coefficients are considered normal non-zero coefficients.

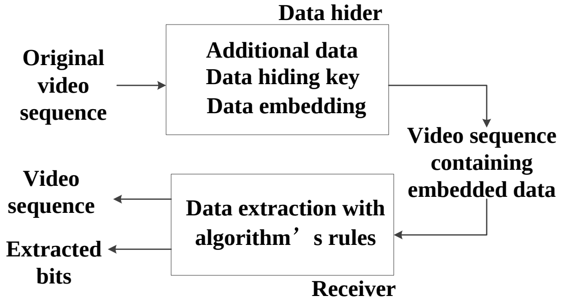


Figure 3: Sketch of proposed scheme.

Here is an example below: 3, 2, 1, 0, 2, -1, 1, -1, 0, 1, -1, 0, 0, 0, 0, 0, where the number of the trailing coefficients is 3, the value is -1, 1, -1 (8th, 10th, and 11ththat were zigzag scanned), and the other coefficients (3rd, 6th, and 7th that were zigzag scanned) are normal non-zero coefficients.

3 Proposed scheme

3.1 Trailing coefficients' application in steganography

Generally speaking, there are 15 kinds of trailing coefficients in DCT blocks, as shown in Table 1. As can be seen from the table, the trailing coefficients' distribution follows certain regularity. As a result of entropy coding, trailing coefficients will not be affected by the compression. Therefore, there is an advantage of selecting trailing coefficients as points in information hiding.

Table 1: 15 kinds of trailing coefficients.

1	none	6	-11	11	-111
2	1	7	-1-1	12	1-1-1
3	-1	8	111	13	-11-1
4	11	9	11-1	14	-1-11
5	1-1	10	1-11	15	-1-1-1

3.2 Embedding algorithm

- **Step 1.** Pretreatment: use K to generate a pseudo-random sequence, p, and preprocess it as the following formula:

$$f_i = m_i \oplus p_i \tag{1}$$

where m_i is the original secret information and f_i is the sequence of post-processing. The purpose is to reduce the correlation of secret information and improve safety. This method can achieve real-time processing;

- **Step 2.** Perform a DCT transform on frames, then traverse all the DCT trailing coefficients and arrange the blocks in order;

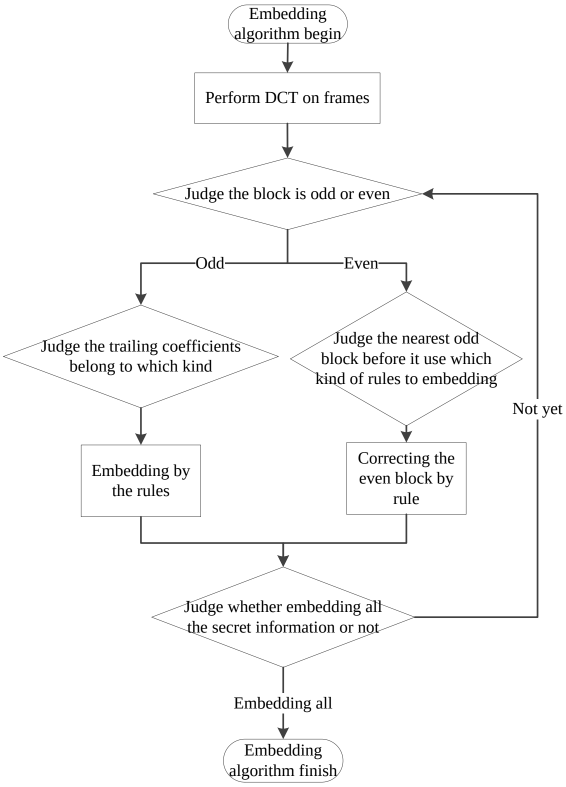

Embedding algorithm begin
Perform DCT on frames
Judge the block is odd or even
Odd
Even
Judge the trailing coefficients belong to which kind
Judge the nearest odd block before it use which kind of rules to embedding
Not yet
Embedding by the rules
Correcting the even block by rule
Judge whether embedding all the secret information or not
Embedding all
Embedding algorithm finish

Figure 4: Flow of embedding algorithm.

- **Step 3.** Use the odd-numbered blocks as embedding blocks and the even-numbered blocks as correcting blocks. Simply speaking, if the current block is embedding secret information, the following block is a correcting block;

- **Step 4.** Embedding process. Determining whether the summary value of trailing coefficients is positive or negative is the key point to our algorithm. We want the value to be negative when the secret information bit is 0, and the value should be positive when the secret information bit is 1. The embedding rules are as follows:

  1. *The embedding rules of the odd blocks.* When the secret information bit is 0, the rule is as shown in Table 2. When secret information bit is 1, the rule is shown in Table 3.

Table 2: The embedding rules when the secret information bit is 0.

1→ -1	-1-1→ -1-1	1-1-1→ 1-1-1
-1→ -1	111→ 1-1-1	-11-1→ -11-1
11→ -1-1	11-1→ 1-1-1	$-1-11 \rightarrow$ -1-11
1-1→ -1-1	1-11→ 1-1-1	$-1-1-1 \rightarrow$ -1-1-1
-11→ -1-1	-111→ -11-1	$0 \rightarrow$ -1

Table 3: The embedding rules when the secret information bit is 0.

1→ 1	-1-1→ 11	$1-1-1 \rightarrow$ 1-11
-1→ 1	111→ 111	$-11-1 \rightarrow$ -111
11→ 11	11-1→ 111	$-1-11 \rightarrow$ -111
1-1→ 11	1-11→ 111	$-1-1-1 \rightarrow$ -111
-11→ 11	-111→ -111	$0 \rightarrow 1$

  As can be seen from the above tables, when modifying the DCT coefficients, the max number that can be modified is 2. When modifying 0, we choose the first 0 scanned by zigzag after the last non-zero numbers; the rest situations in Table 2 and Table 3 are only modified a number or without modification, so the algorithm can achieve better security.

  2. *The rules of even blocks for correcting.* When an odd block has been modified, we will use the next even block to correct. If we change -1 to 1 to embed the secret, then we change the last 1 of a correction block to -1. If there is no existing1 in the correcting block, we change the first 0 bit which after the last non-zero numbers to -1. In the odd block, if we change 1 to -1, then we change the last -1 in the correcting block to 1; if there is no existing -1 in the correction block, change the first 0 bit which after the last non-zero numbers to 1.If we change 0 to 1 in odd block to hide the secret information, then the last 1 in the corrected block is changed to 0; if there is no existing 1, nothing is modified; if we change 0 to -1 in the modified block to hide the secret information, the last -1 in corrected block is changed to 0; if there is no existing -1, nothing is modified; the purpose of this correction is to hold the histogram between stego-DCT coefficients' and cover-DCT coefficients';

- **Step 5.** Repeating Step 4, until all the secret information is embedded. The flow of the embedding algorithm is show in Figure 4.

3.3 Extraction algorithm

- **Step 1.** Perform a DCT transformation on frames, and traverse all the DCT trailing coefficients, then arrange the blocks in order;

- **Step 2.** Follow the rules of extracting, based on the following Formula:

$$m_i = \begin{cases} 0, & if \;\; S(j) < 0 \; and \; j \bmod 2 = 1 \\ 1, & if \;\; S(j) > 0 \; and \; j \bmod 2 = 1 \end{cases} \qquad (2)$$

  Where m_i is the secret information bit, j is the order of the DCT block based on Step 1, and $S(j)$ is the sum-value ofthe trailing coefficients;

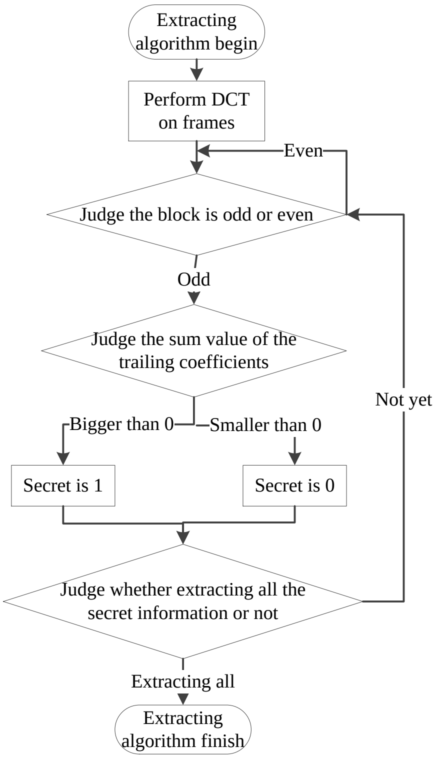

Extracting algorithm begin
Perform DCT on frames
Even
Judge the block is odd or even
Odd
Judge the sum value of the trailing coefficients
Bigger than 0
Smaller than 0
Secret is 1
Secret is 0
Not yet
Judge whether extracting all the secret information or not
Extracting all
Extracting algorithm finish

Figure 5: Flow of the extracting algorithm.

- **Step 3.** Repeat Step 2 until all the secret information is extracted;

- **Step 4.** Inverse pretreatment; the rules are shown in the following Formula:

$$m_i = f_i \oplus p_i \tag{3}$$

Where m_i is the original secret information and f_i is the sequence of extracting information. The flow of the extracting algorithm is shown in Figure 5.

4 Experimental results and analysis

Our experimental environment is based on X.264, VC++ 2008, and Matlab2008. The video sequences are downloaded from the website, "media.xiph.org". Each sequence is 15 frames/s, the bit rate is 396kbit/s, and the format is QCIF (News, Mobile), CIF (Container, Carphone). The secret information is the image "lena.bmp."

4.1 Theoretical analysis

The probability that changes the coefficient -1 to 1 can be expressed as follows:

$$\begin{aligned}
&P((-1) \to (1)) = p(m(i) = 1)\{p((-1) \to (1)) \\
&+ p((1,-1) \to (1,1)) + p((-1,1) \to (1,1)) \\
&+ 2p((-1,-1) \to (1,1)) \\
&+ p((1,-1,-1) \to (1,-1,1)) \\
&+ p((-1,1,-1) \to (-1,1,1)) \\
&+ p((1,-1,1) \to (-1,1,1)) \\
&+ 2p((-1,-1,-1) \to (-1,1,1)) + p((0) \to (1))\} \\
&+ p(m(i) = 0)\{0\}
\end{aligned} \tag{4}$$

The probability that changes the coefficient 1 to -1 can be expressed as follows:

$$\begin{aligned}
&P((1) \to (-1)) = p(m(i) = 0)\{p((1) \to (-1)) \\
&+ p((1,-1) \to (-1,-1)) + p((-1,1) \to (-1,-1)) \\
&+ 2p((1,1) \to (-1,-1)) \\
&+ 2p((1,1,1) \to (1,-1,-1)) \\
&+ p((1,1,-1) \to (1,-1,-1)) \\
&+ p((1,-1,1) \to (1,-1,-1)) \\
&+ p((-1,1,1) \to (-1,1,-1))\} \\
&+ p(m(i) = 1)\{0\}
\end{aligned} \tag{5}$$

Since the secret information is encrypted, the probability of 0 and 1 remains the same, as shown below:

$$p(m(i) = 1) = p(m(i) = 0) \tag{6}$$

We can conclude from formula (4),formula (5), and formula (6), that we can obtain the probability $p((1) \to (-1)) = p((-1) \to (1))$. Therefore, this method can achieve high security.

4.2 Analysis of invisibility

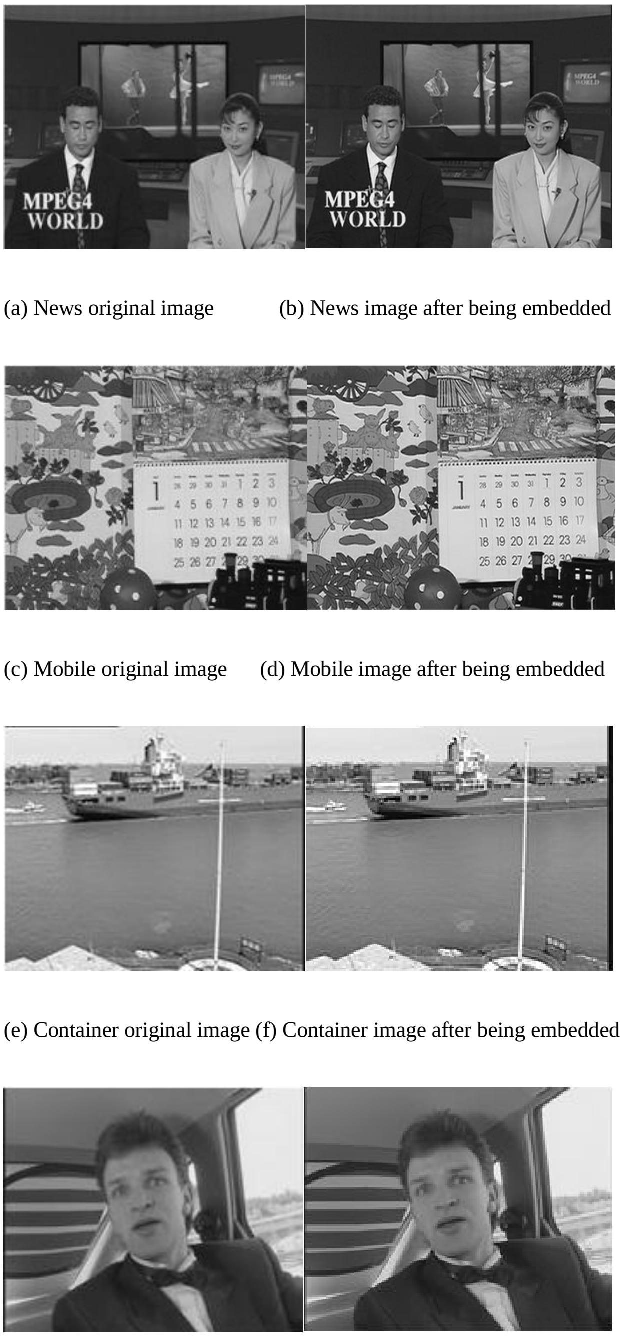
4.2.1 Subjective analysis of visibility

The original and embedded frames of test sequences are shown in Figure 6. As can be seen, there is no significant difference between them. So, we can conclude that our algorithm is better in terms of visibility.

4.2.2 Objective analysis of visibility

The PSNR value is the key to judging the visibility. According to the HVS,when the PSNR value is above 30dB, the sequence is clear and fluent. The PSNR value of the test sequence has been shown in Table 4, and the results show that the decrease is low after embedding, and the average decline of the PSNR value is about 1.156dB.

Since the Carphone sequence is rich in texture blocks, and there are also many smoothing blocks, we calculate out pre-30 frames' PSNR value of it. Figure 7 shows the PSNR



(a) News original image (b) News image after being embedded

(c) Mobile original image (d) Mobile image after being embedded

(e) Container original image (f) Container image after being embedded

(g) Carphone original image (h) Carphone image after being embedded

Figure 6: Comparison on the original and embedded frames of test sequences.

Table 4: Comparison of PSNR values before and after embedding.

Test sequence	Original PSNR value/dB	PSNR value after embedding/dB	Decrease /dB
News	36.743	35.945	0.798
Mobile	35.376	34.347	1.029
Container	36.232	35.089	1.143
Carphone	35.798	34.141	1.657

value of the pre-30 frames of Carphone after embedding secret information. As can be seen, the impact of the first frame is about 2.27dB, and the impact of the No.16 frame is about 1.89dB; the other frames are not affected much.

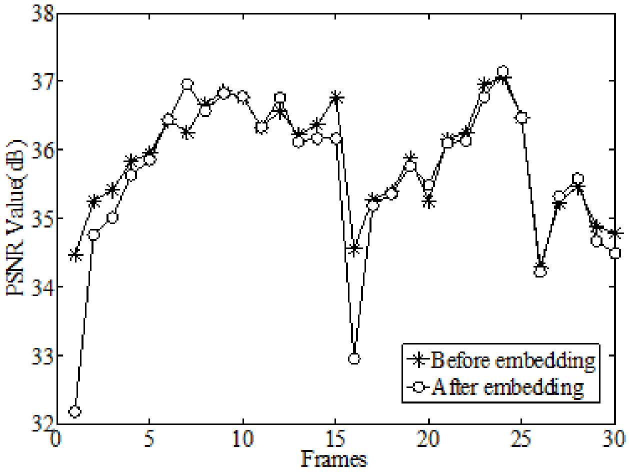


Figure 7: Video image and extraction of the secret information image after attack.

4.3 Steganographic capacity

Reference [16] proposed a steganographic algorithm based on modifying the DCT coefficients, and reference [19] also proposed an algorithm based on modifying the DCT coefficients for hiding, so we use these two references to be compared with our algorithm.

As can be seen from Figure 8, our algorithm's capacity has been improved.Because of our algorithm embedding secret information in half of the DCT blocks, it can achieve an improved capacity.

4.4 Robustness testing

The main goal of the robustness test of the steganographic algorithm is to detect anti-attack capability. For this test, we use salt and pepper noise and Gaussian low-pass filtering.

In the experiment, we add salt and pepper noise to the video sequence, and the intensity is 0.05; Figure 9 shows

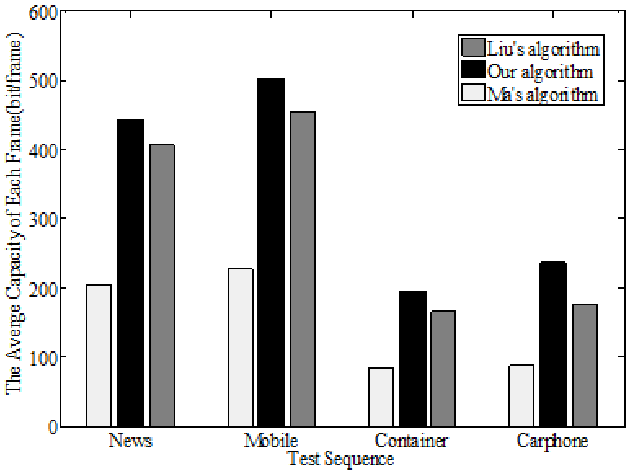


Figure 8: Video image and extraction of the secret information after attack.

the effect it has on News and the secret information image we extract.

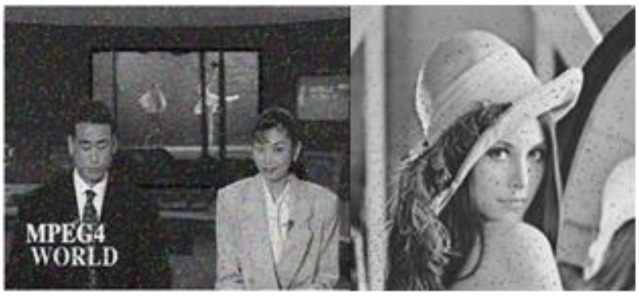


Figure 9: Video image and extraction of the secret information image after attack.

Figure 10 represents the experiment after a 3 × 3 Gaussian low-pass filter, the effect on Mobile, and the secret information image we extract.

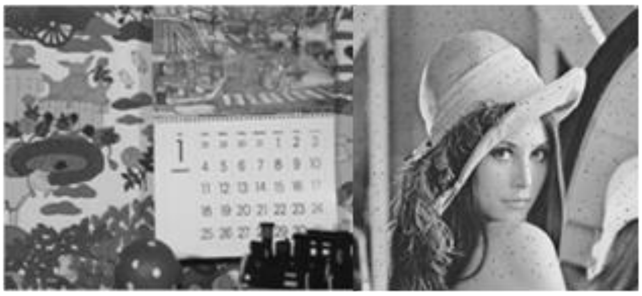


Figure 10: Video image and extraction of the secret information after attack.

Table 5 is the SIM value between the secret information after attack and the original one. The formula of SIM is as follows:

$$SIM(X,Y) = \frac{\sum_i X(i)Y(i)}{\sqrt{\sum_i X(i)^2}\sqrt{\sum_i Y(i)^2}} \qquad (7)$$

In the formula, $X(i)$ and $Y(i)$ represent the original image and the stego-image to be evaluated in the one-dimensional sequence of pixel values respectively; $SIM \in (0,1]$ takes the value of 1 only when the images we compared are exactly the same.

Table 5: The SIM value of extracting secret information after attack.

Video sequence	Add salt and pepper noise	Add Gaussian low-pass filtering
News	0.827	0.899
Mobile	0.846	0.943
Container	0.813	0.921
Carphone	0.790	0.906

Figure 9, Figure 10, and Table 5 indicate that the algorithm has high robustness and anti-attack capability.

4.5 Steganalysis detection

Heidari has proposed a steganalysis algorithm [20], and it has a high detection rate for the steganography algorithm based on modifying the DCT coefficients. Therefore, our video sequence would be extracted for each frame, and we then we test the detection rate of every frame.

A false positive (FP) represents classifying the non-stego frames as stego frames. A false negative (FN) indicates classifying the stego framesas non-stego frames [21]. The results can be shown in Table 6:

Table 6: The results of using Heidari's algorithm.

Video	FP (%)	FN (%)	Error rate(%)
News	53.45	48.12	50.79
Mobile	46.51	45.08	45.80
Container	52.67	49.59	51.13
Carphone	47.75	40.64	44.20

Generally, the higher the FN and FP is, the better the steganographic algorithm is. As can be seen from Table 6, when detecting our algorithm,FP and FN are high.

5 Conclusion and discussion

In the past, transmitting a huge video sequence would take a great amount of time, so the video sequence is not common in steganography.Usually,the image is used as the cover carrier, but it also limits the information bit that is to be hidden. However, a high speed network offers a platform to transmit large multimedia, so we can use it to hide more information than before.

This paper proposed a video steganography algorithm based on trailing coefficients in a high speed network, and we modified the value of trailing coefficients to make sure that when the secret information bit is 0, the sum value is negative, and when the secret information bit is 1, the sum value is positive. In order to ensure that the DCT coefficients of the cover video after embedding have been changed, the algorithm used the method that modified the odd-numbered blocks to hide and modified the even-numbered blocks to correct. The experimental results indicated that our algorithm has little impact on the video's visual invisibility, the capacity of steganography is improved, and it has high robustness. Therefore, our research has better performance compared to previous algorithms.

Although this paper has proposed a scheme to protect the security of a high-speed network, and our algorithm can achieve some good features as mentioned before, some problems should also be discussed.For example, if we hide secret information in images or videos, no method to completely recover the hidden media has been found. In future studies, there will be a focus on revising the process of hiding information.

The next inadequacy of our method is that we did not use the protocol of a high-speed network; if we hide information in it, we will raise the capacity greatly and increase the cost of bandwidth. In future studies, the goal will be to find a method of hiding information in the protocol of networks, but without greatly increasing the cost of bandwidth.

Acknowledgment

The authors would like to thank the anonymous reviewers for the constructive comments. This work was supported by the National Science Foundation of China: Theory research on extracting and optimizing feature of image steganalysis (Grant No.61379152). And it was also supported by the National Science Foundation of China: Cross-Domain Human Action Recognition by Knowledge Transfer (Grant No.61403417).

References

[1] H. G. Zhang, R. Y. Du, J. M. Fu, B. Zhao, L. N. Wang. (2014) *Information security: an independent discipline a new subject.* Information and Communication Security, no.5 (in Chinese).

[2] H. J. Bi (2005). *A New Generation of Video Compression Standard—H.264/AVC.* Beijing: Posts & Telecom Press, pp. 110-111 (in Chinese).

[3] R. J. Mstafa, K. M.Elleithy (2014). *A Highly Secure Video Steganography using Hamming Code (7, 4).* 2014 IEEE Long Island Systems, Applications and Technology Conference (LISAT), pp.1 - 6.

[4] M. M. Sadek, A. S.Khalifa, M. G. M.Mostafa (2014). *Video steganography: a comprehensive review.* Multimedia Tools & Applications, vol.74, pp.1-32.

[5] J. Ridgway, M. Stannett (2014). *Developing a Video Steganography Toolkit.* Eprint Arxiv.

[6] K. P. Divya, K. Mahesh (2014). *Random Image Embedded in Videos using LSB Insertion Algorithm.* International Journal of Engineering Trends & Technology, vol. 13, no.8, pp.381-385.

[7] K. Churin, J. Preechasuk, C. Chantrapornchai (2013). *Exploring Video Steganography for Hiding Images Based on Similar Lifting Wavelet Coefficients.* Advances in Information Technology. Springer International Publishing, vol. 409, pp.35-46.

[8] H. Gupta, S. Chaturvedi (2014). *Video Steganography through LSB Based Hybrid Approach.* International Journal of Computer Science and Network Security (IJCSNS), vol.14, no.3, pp. 99-106.

[9] Y. Shen, Q. Pei, Q. Xu, Z, Zhang (2012). *The multimedia service session handoff method in heterogeneous wireless networks.* International Journal of Grid and Utility Computing, vol. 3, no. 1, pp. 68-77.

[10] D. V. Bernardo, D. B. Hoang (2012). *Multi-layer security analysis and experimentation of high speed protocol data transfer for GRID.* International Journal of Grid and Utility Computing, vol. 3, no. 2/3, pp. 81-88.

[11] Y. Wang; J. Du; X. Cheng; Z. Liu; K. Lin (2016). *Degradation and encryption for outsourced PNG images in cloud storage.* International Journal of Grid and Utility Computing, vol. 7, no. 1, pp. 22-28.

[12] J. Kolodziej, F. Xhafa (2011). *Supporting situated computing with intelligent multi-agent systems.* International Journal of Space-Based and Situated Computing, vol. 1, no. 1, pp. 30-42.

[13] R. Pereira, E. G. Pereira (2016). *Future internet: trends and challenges.* International Journal of Space-Based and Situated Computing, vol. 5, no. 3, pp. 159-167.

[14] G. L. Hua, Z. B. Li, B. Feng (2013). *Low frequency steganography algorithm for H.264/AVC.* Journal on Communications, vol. 34, no. Z2, pp. 47-50.

[15] G. C. Langelaar, R. R. Lagendijk (2001). *Optimal differential energy watermarking of DCT encode images and video.* IEEE Transactions on Image Processing, vol. 10, no.1, pp. 148-158.

[16] X. J. Ma (2010). *The Research on Video Data Hiding Algorithms Based on H.264/AVC.* Huazhong Univercity of Science and Technology (in Chinese).

[17] X. S. He, Z. Luo (2008). *A Novel Steganographic Algorithm Based on the Motion Vector Phase.* International Conference on Computer Science and Software Engineering CSSE, Wuhan, China, pp. 822-825.

[18] W. W. Zhang, R. Zhang, Y. J. Liu , et al (2012). *Robust Video Watermarking Algorithm for H.264/AVC Based on Texture Feature.* . Journal on Communications, vol. 33, no.3, pp. 82-89 (in Chinese).

[19] C. H. Liu, O. T. Chen (2008). *Data Hiding in Intra Prediction Modes of H.264/AVC*. IEEE International Symposium on Circuits and Systems, pp.3025-3028.

[20] Heidari, Mortaza, G.Shahrokh (2013). *Universal image steganalysisusing singular values of DCT coefficients.* 10th International ISC Conference on Information Security and Cryptology (ISCISC), Yazd, Iran, pp.1-5.

[21] T. Filler, J. Judas, J. Fridrich (2011). *Minimizing additive distortion in steganography using syndrome-trellis codes.* IEEE Transactions on Information Forensics and Security, vol. 6, no.3, pp. 920-935.